**3GPP TSG-SA3 Meeting #104-e *S3-212565***

**e-meeting, 16 - 27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1154** | **rev** | **-** | **Current version:** | **17.2.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Storage of Kausf |
|  |  |
| ***Source to WG:*** | NEC |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-08-06 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | CR agreed in last meeting for rel-17 mandates SMC procedure after authentication procedure. When the UE receives Security mode command message after the authentication procedure then the UE stores the Kausf created during the primary authentication procedure. Legacy network does not mandatorily initiate SMC procedure. When the rel-17 UE is registers to the legacy network then after the Authentication procedure the rel-17 UE will wait for the SMC message to stores the Kausf but legacy AMF may not not send the SMC message. In this case the rel-17 will not stores the Kausf in absence of the SMC message.  |
|  |  |
| ***Summary of change:*** | Network sends an indicator to the UE in the registration accept message that it mandatorily sends SMC message after authentication procedure.  |
|  |  |
| ***Consequences if not approved:*** | The Rel-17 UE will not stores the Kausf in legacy network. |
|  |  |
| ***Clauses affected:*** | 6.1.3.2.0 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

##### 6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.



Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

1. For each Nudm\_Authenticate\_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [9]. The UDM/ARPF shall then derive KAUSF (as per Annex A.2) and calculate XRES\* (as per Annex A.4). Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES\*, and KAUSF.

2. The UDM shall then return the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G AKA in a Nudm\_UEAuthentication\_Get Response. In case SUCI was included in the Nudm\_UEAuthentication\_Get Request, UDM will include the SUPI in the Nudm\_UEAuthentication\_Get Response after deconcealment of SUCI by SIDF.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication in the Nudm\_UEAuthentication\_Get Response.

3. The AUSF shall store the XRES\* temporarily together with the received SUCI or SUPI.

4. The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES\* from XRES\* (according to Annex A.5) and KSEAF from KAUSF(according to Annex A.6), and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G HE AV.

5. The AUSF shall then remove the KSEAF and return the 5G SE AV (RAND, AUTN, HXRES\*) to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response.

6. The SEAF shall send RAND, AUTN to the UE in a NAS message Authentication Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM. . This message also includes a SMC capability indicator indicating that the SEAF mandatorily executes the security mode command procedure after the successful authentcaiton procedure.

NOTE 2: The ABBA parameter is included to enable the bidding down protection of security features.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102[9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES\* from RES according to Annex A.4. The ME shall calculate KAUSF from CK||IK according to clause A.2. The ME shall calculate KSEAF from KAUSF according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN. If the UE received the SMC capability indicator in step 7, the UE shall wait for the security mode command message before storing the Kausf created during the authentication procedure.

NOTE 3: This separation bit in the AMF field of AUTN cannot be used anymore for operator specific purposes as described by TS 33.102 [9], Annex F.

8. The UE shall return RES\* to the SEAF in a NAS message Authentication Response.

9. The SEAF shall then compute HRES\* from RES\* according to Annex A.5, and the SEAF shall compare HRES\* and HXRES\*. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in sub-clause 6.1.3.2.2. If the UE is not reached, and the RES\* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.

10. The SEAF shall send RES\*, as received from the UE, in a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF.

11. When the AUSF receives as authentication confirmation the Nausf\_UEAuthentication\_Authenticate Request message including a RES\* it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF shall store the KAUSF. AUSF shall compare the received RES\* with the stored XRES\*. If the RES\* and XRES\* are equal, the AUSF shall consider the authentication as successful from the home network point of view. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for linking with the authentication confirmation).

NOTE 4: It is left to implementation to temporarily store the KAUSF received in step 2 in AUSF until the RES\* verification is done successfully (i.e., at step 11).

12. The AUSF shall indicate to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the KSEAF shall be sent to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response. In case the AUSF received a SUCI from the SEAF in the authentication request (see sub-clause 6.1.2 of the present document), and if the authentication was successful, then the AUSF shall also include the SUPI in the Nausf\_UEAuthentication\_Authenticate Response message.

If the authentication was successful, the key KSEAF received in the Nausf\_UEAuthentication\_Authenticate Response message shall become the anchor key in the sense of the key hierarchy as specified in sub-clause 6.2 of the present document. Then the SEAF shall derive the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7. The SEAF shall provide the ngKSI and the KAMF to the AMF. If the AUSF indicates that the authentication was successful from the home network point of view, then the AMF shall initiate NAS security mode command procedure (see clause 6.7.2) with the UE, to take the newly generated partial native 5G NAS security context into use. Upon receiving the valid NAS Security Mode Command message from the AMF, the UE shall consider the performed primary authentication as successful.

If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and KAMF to the AMF after it has received the Nausf\_UEAuthentication\_Authenticate Response message containing KSEAF and SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.